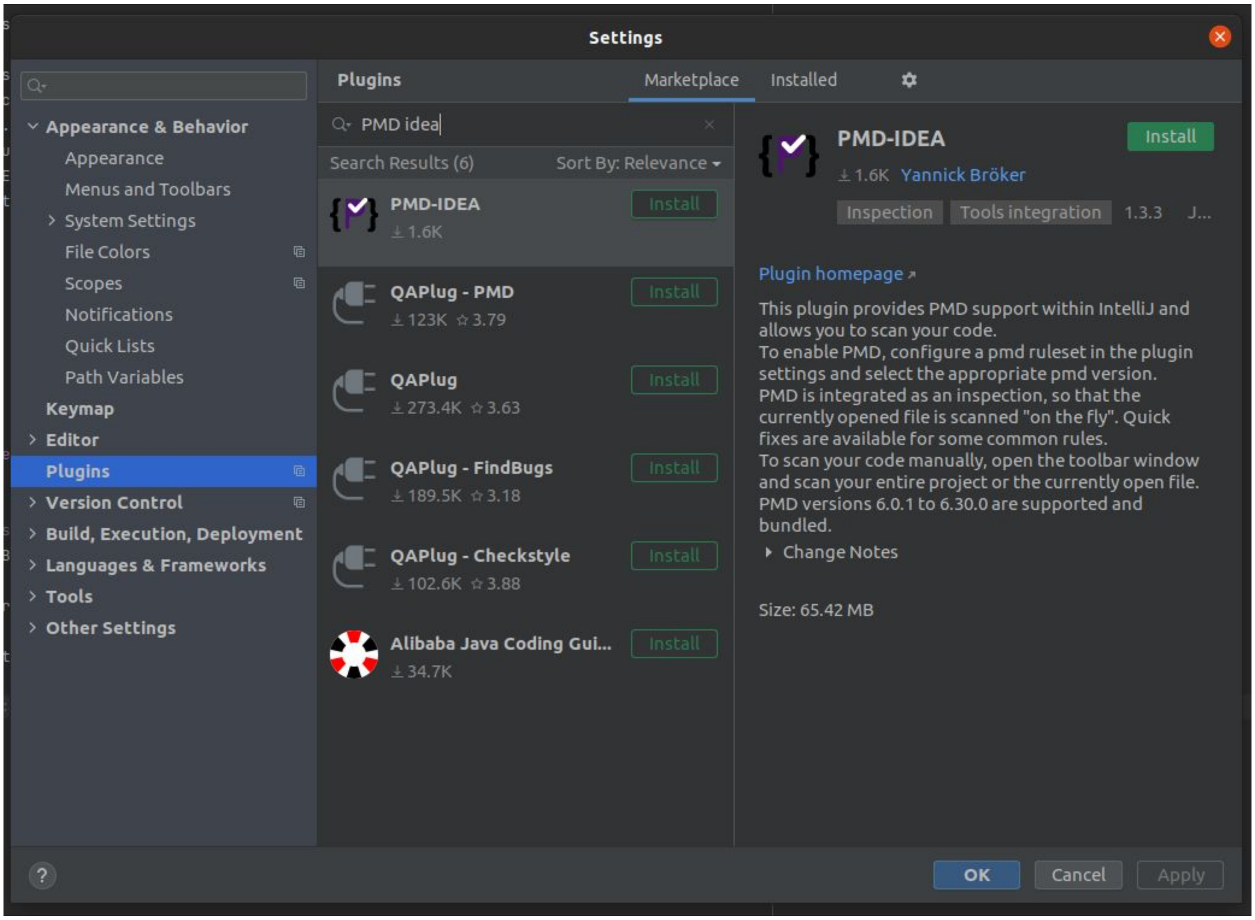
Code Quality Java
Spring AU 2021

Ajay S ajay.s@accolitedigital.com

---

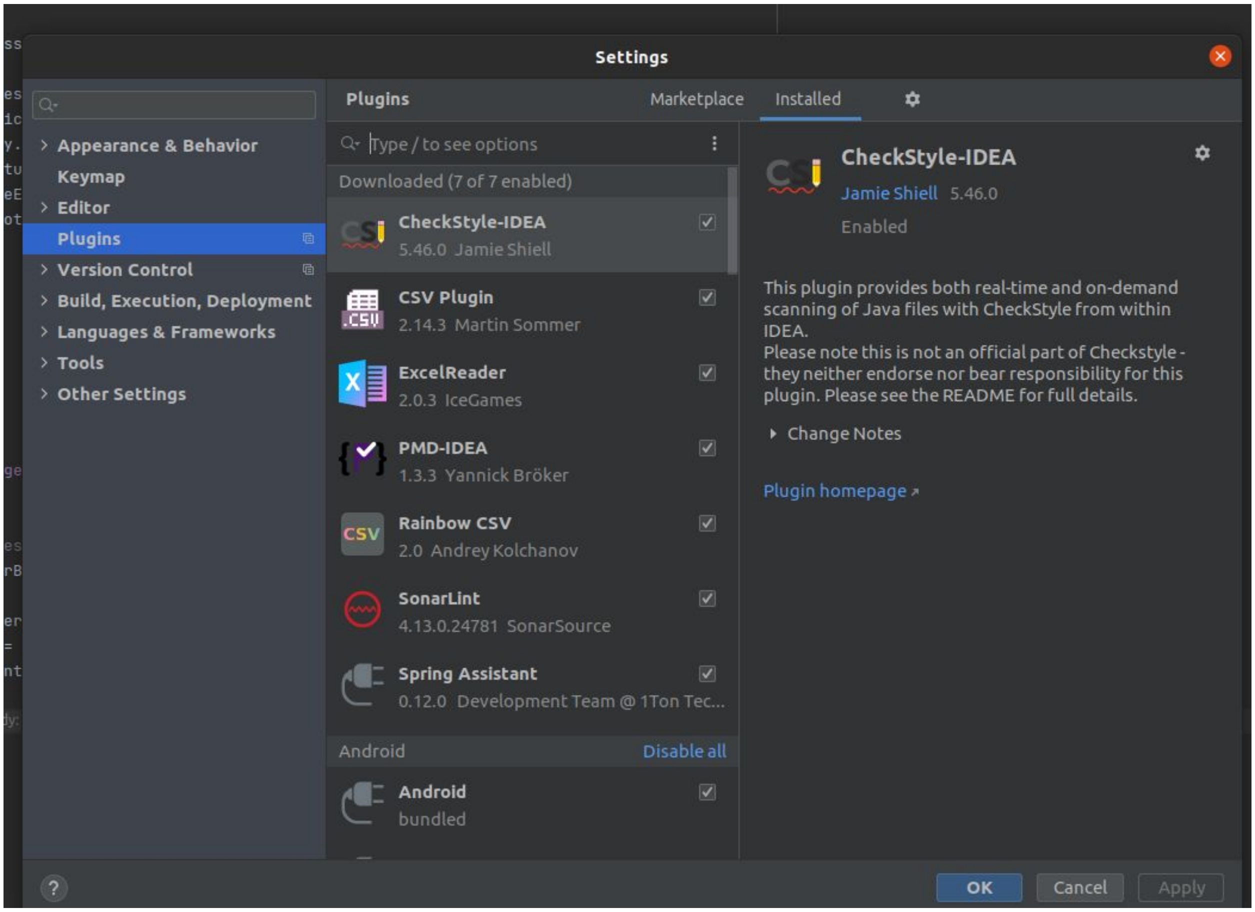
1. Code Quality Plugins
IDE: Intellij

Plugin installation marketplace



This plugin provides PMD support within IntelliJ and allows you to scan your code.
To enable PMD, configure a pmd ruleset in the plugin settings and select the appropriate pmd version.
PMD is integrated as an inspection, so that the currently opened file is scanned "on the fly". Quick fixes are available for some common rules.
To scan your code manually, open the toolbar window and scan your entire project or the currently open file.
PMD versions 6.0.1 to 6.30.0 are supported and bundled.

Installed plugins



Downloaded (7 of 7 enabled)

- ☑ CheckStyle-IDEA 5.46.0 Jamie Shiell
- ☑ CSV Plugin 2.14.3 Martin Sommer
- ☑ ExcelReader 2.0.3 IceGames
- ☑ PMD-IDEA 1.3.3 Yannick Bröker
- ☑ Rainbow CSV 2.0 Andrey Kolchanov
- ☑ SonarLint 4.13.0.24781 SonarSource
- ☑ Spring Assistant 0.12.0 Development Team @ 1Ton Tec...

Android — Disable all

- ☑ Android bundled

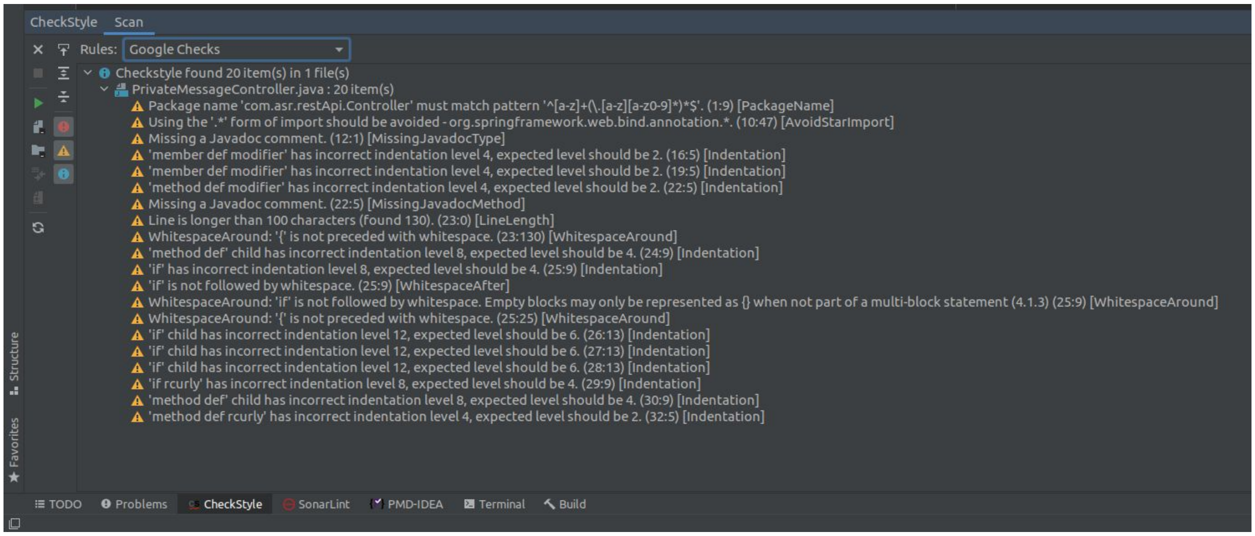
CheckStyle-IDEA
Jamie Shiell 5.46.0
Enabled

This plugin provides both real-time and on-demand scanning of Java files with CheckStyle from within IDEA.
Please note this is not an official part of Checkstyle - they neither endorse nor bear responsibility for this plugin. Please see the README for full details.

Change Notes

Plugin homepage ↗

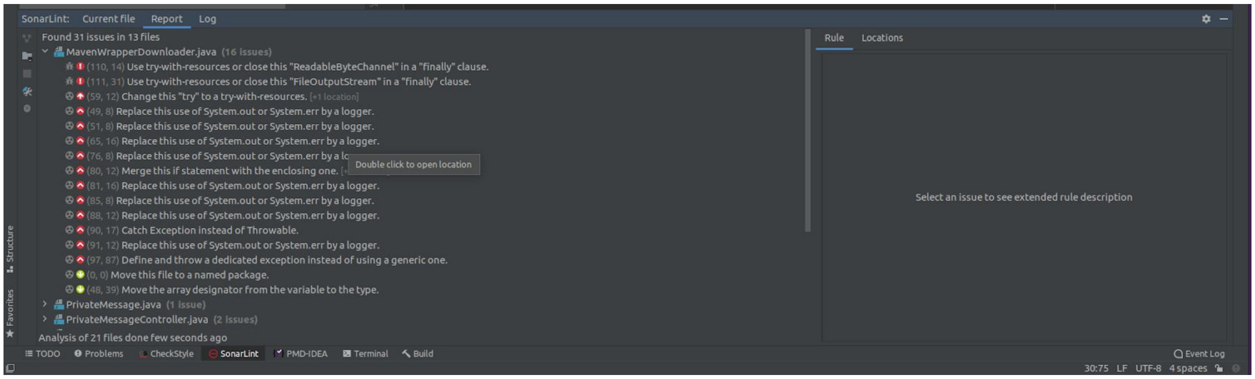
Checkstyle report



Rules: Google Checks

```
Checkstyle found 20 item(s) in 1 file(s)
  PrivateMessageController.java : 20 item(s)
    Package name 'com.asr.restApi.Controller' must match pattern '^[a-z]+(\.[a-z][a-z0-9]*)*$'. (1:9) [PackageName]
    Using the '.*' form of import should be avoided - org.springframework.web.bind.annotation.*. (10:47) [AvoidStarImport]
    Missing a Javadoc comment. (12:1) [MissingJavadocType]
    'member def modifier' has incorrect indentation level 4, expected level should be 2. (16:5) [Indentation]
    'member def modifier' has incorrect indentation level 4, expected level should be 2. (19:5) [Indentation]
    'method def modifier' has incorrect indentation level 4, expected level should be 2. (22:5) [Indentation]
    Missing a Javadoc comment. (22:5) [MissingJavadocMethod]
    Line is longer than 100 characters (found 130). (23:0) [LineLength]
    WhitespaceAround: '{' is not preceded with whitespace. (23:130) [WhitespaceAround]
    'method def' child has incorrect indentation level 8, expected level should be 4. (24:9) [Indentation]
    'if' has incorrect indentation level 8, expected level should be 4. (25:9) [Indentation]
    'if' is not followed by whitespace. (25:9) [WhitespaceAfter]
    WhitespaceAround: 'if' is not followed by whitespace. Empty blocks may only be represented as {} when not part of a multi-block statement (4.1.3) (25:9) [WhitespaceAround]
    WhitespaceAround: '{' is not preceded with whitespace. (25:25) [WhitespaceAround]
    'if' child has incorrect indentation level 12, expected level should be 6. (26:13) [Indentation]
    'if' child has incorrect indentation level 12, expected level should be 6. (27:13) [Indentation]
    'if' child has incorrect indentation level 12, expected level should be 6. (28:13) [Indentation]
    'if rcurly' has incorrect indentation level 8, expected level should be 4. (29:9) [Indentation]
    'method def' child has incorrect indentation level 8, expected level should be 4. (30:9) [Indentation]
    'method def rcurly' has incorrect indentation level 4, expected level should be 2. (32:5) [Indentation]
```

Sonarlint report

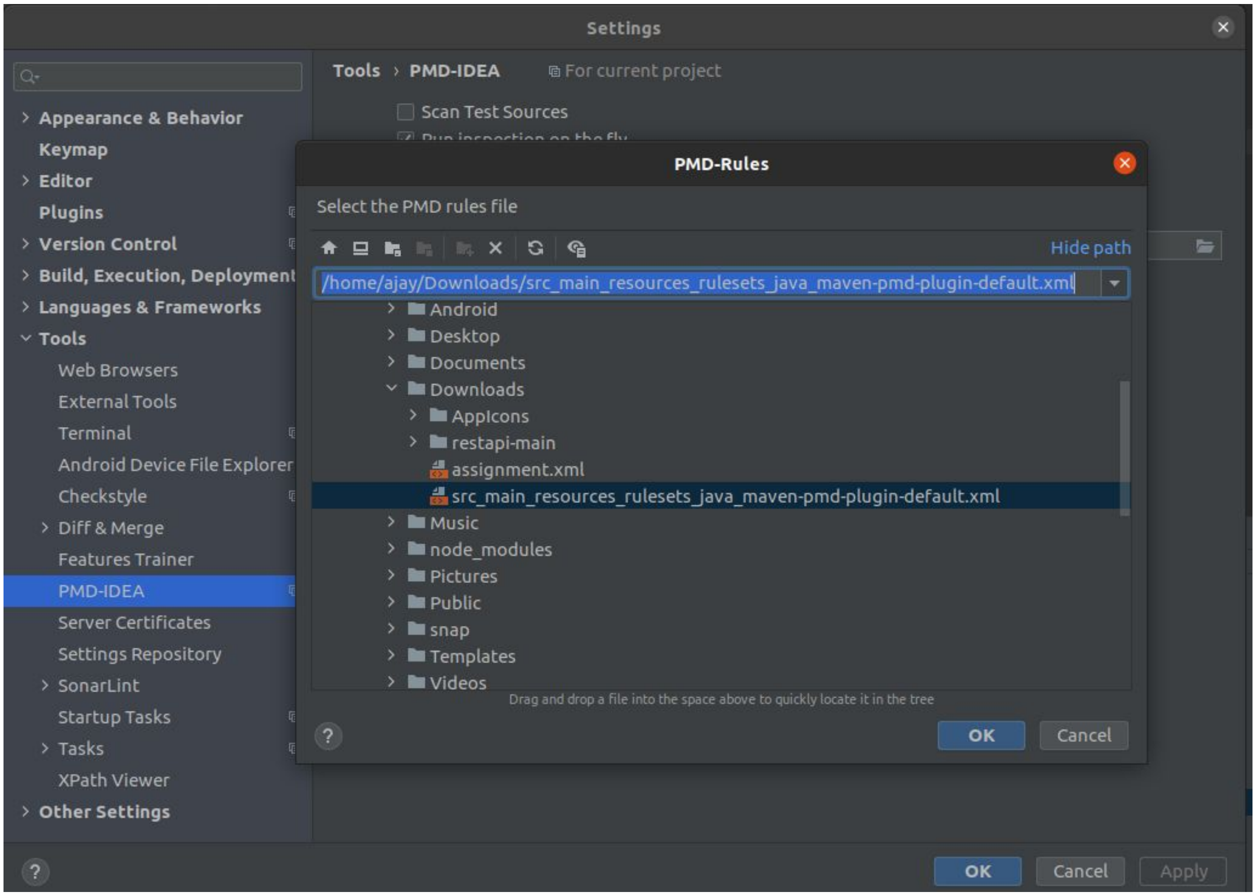


```
Found 31 issues in 13 files
MavenWrapperDownloader.java (16 issues)
    (110, 14) Use try-with-resources or close this "ReadableByteChannel" in a "finally" clause.
    (111, 31) Use try-with-resources or close this "FileOutputStream" in a "finally" clause.
    (59, 12) Change this "try" to a try-with-resources. [+1 location]
    (49, 8) Replace this use of System.out or System.err by a logger.
    (51, 8) Replace this use of System.out or System.err by a logger.
    (65, 16) Replace this use of System.out or System.err by a logger.
    (76, 8) Replace this use of System.out or System.err by a lc
    (80, 12) Merge this if statement with the enclosing one. [+
    (81, 16) Replace this use of System.out or System.err by a logger.
    (85, 8) Replace this use of System.out or System.err by a logger.
    (88, 12) Replace this use of System.out or System.err by a logger.
    (90, 17) Catch Exception instead of Throwable.
    (91, 12) Replace this use of System.out or System.err by a logger.
    (97, 87) Define and throw a dedicated exception instead of using a generic one.
    (0, 0) Move this file to a named package.
    (48, 39) Move the array designator from the variable to the type.
PrivateMessage.java (1 issue)
PrivateMessageController.java (2 issues)
Analysis of 21 files done few seconds ago
```

Double click to open location

Select an issue to see extended rule description

PMD select ruleset file (file is uploaded separately)



□ Scan Test Sources

☑ Run inspection on the fly

PMD-Rules

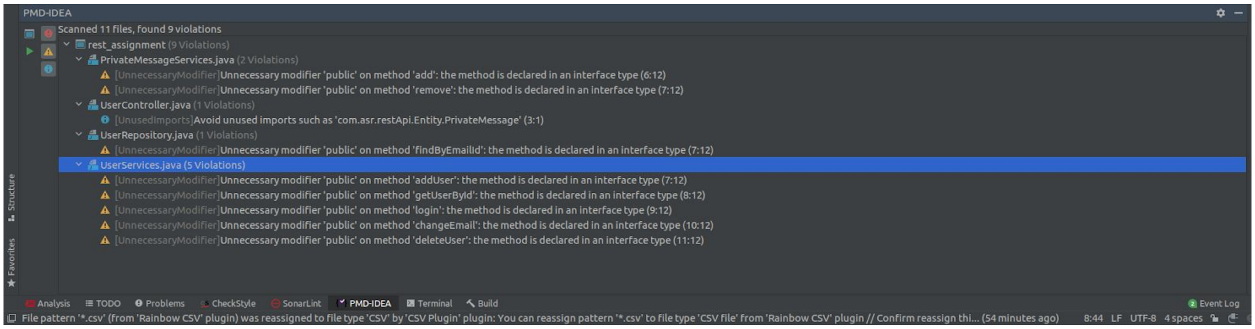
Select the PMD rules file

/home/ajay/Downloads/src_main_resources_rulesets_java_maven-pmd-plugin-default.xml

```
> Android
> Desktop
> Documents
v Downloads
    > AppIcons
    > restapi-main
      assignment.xml
      src_main_resources_rulesets_java_maven-pmd-plugin-default.xml
> Music
> node_modules
> Pictures
> Public
> snap
> Templates
> Videos
```

Drag and drop a file into the space above to quickly locate it in the tree

PMD report



```
Scanned 11 files, found 9 violations
  rest_assignment (9 Violations)
    PrivateMessageServices.java (2 Violations)
      [UnnecessaryModifier]Unnecessary modifier 'public' on method 'add': the method is declared in an interface type (6:12)
      [UnnecessaryModifier]Unnecessary modifier 'public' on method 'remove': the method is declared in an interface type (7:12)
    UserController.java (1 Violations)
      [UnusedImports]Avoid unused imports such as 'com.asr.restApi.Entity.PrivateMessage' (3:1)
    UserRepository.java (1 Violations)
      [UnnecessaryModifier]Unnecessary modifier 'public' on method 'findByEmailId': the method is declared in an interface type (7:12)
    UserServices.java (5 Violations)
      [UnnecessaryModifier]Unnecessary modifier 'public' on method 'addUser': the method is declared in an interface type (7:12)
      [UnnecessaryModifier]Unnecessary modifier 'public' on method 'getUserById': the method is declared in an interface type (8:12)
      [UnnecessaryModifier]Unnecessary modifier 'public' on method 'login': the method is declared in an interface type (9:12)
      [UnnecessaryModifier]Unnecessary modifier 'public' on method 'changeEmail': the method is declared in an interface type (10:12)
      [UnnecessaryModifier]Unnecessary modifier 'public' on method 'deleteUser': the method is declared in an interface type (11:12)
```

```
File pattern '*.csv' (from 'Rainbow CSV' plugin) was reassigned to file type 'CSV' by 'CSV Plugin' plugin: You can reassign pattern '*.csv' to file type 'CSV file' from 'Rainbow CSV' plugin // Confirm reassign thi... (54 minutes ago)    8:44  LF  UTF-8  4 spaces
```

2. **Secure coding standards**
   1. **CWE - Common Weakness Enumeration**

      It's a list of common software and hardware security weakness.

      2020 Top few CWE list
      - **Cross-site scripting**
      - **SQL injection**
      - **Cross-site Request Forgery**
      - **Improper Authentication**
      - **Null Pointer dereference**
   2. **OWASP top 10**

      The Open Web Application Security Project

      A community which provides documentation and tools for web app security

      Few of the top OWASP security risks
      - **Injection**
      - **Broken Authentication**
      - **Sensitive Data Exposure**
      - **XML External Entities**
      - **Broken Access Control**
   3. **CERT**

      A secure coding standard with a risk assessment for violations

      Aims to provide security and code quality

CERT Risk assessment
Each has a value between 1 - 3
1 - lowest

1. **Severity**
2. **Likelihood**
3. **Remediation cost**

The above 3 are grouped together to determine the level of vulnerability

Level	Priorities	Interpretation
L1	12, 18, 27	Severity: High Severity Likelihood: Likely Remediation Cost: Inexpensive to Repair
L2	6, 8, 9	Severity: Medium Severity Likelihood: Probable Remediation Cost: Medium Cost to Repair
L3	1, 2, 3, 4	Severity: Low Severity Likelihood: Unlikely Remediation Cost: Expensive to Repair

c. SANS 25

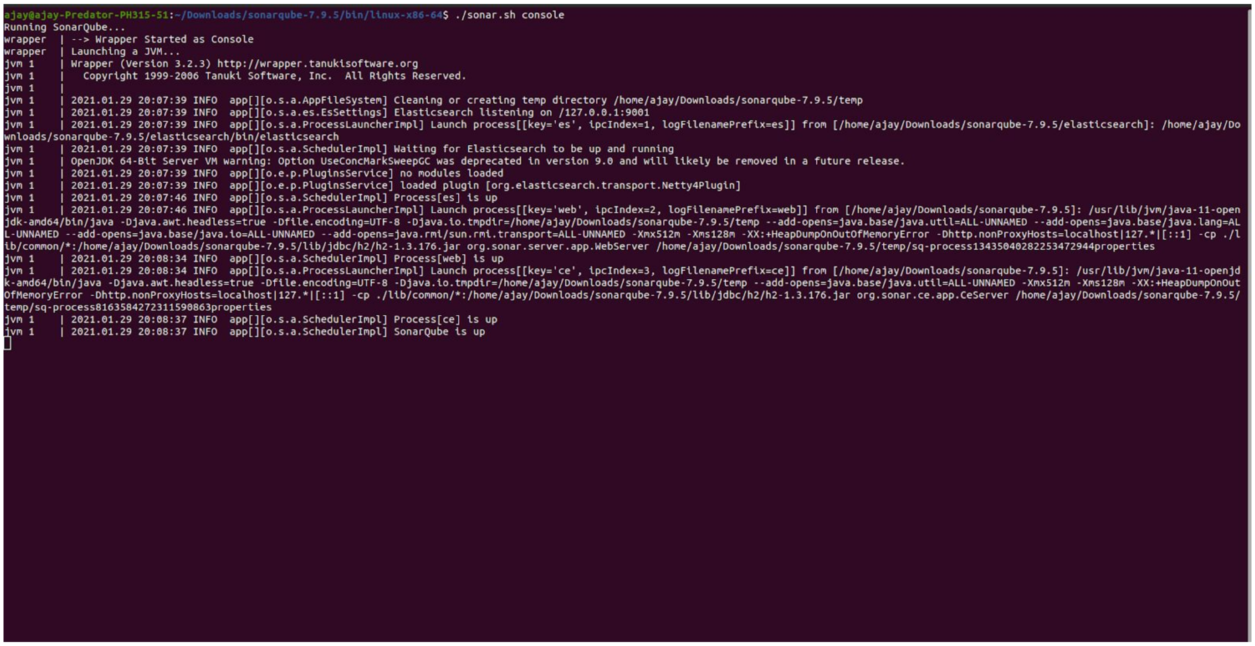
It’s a list of top 25 CWE. It is also a netsparker standard which can be used while scanning the website for vulnerabilities

Few of the top SANS 25

- **Use of hardcoded credentials**
- **Uncontrolled resource consumption**
- **Improper privilege management**
- **Improper certificate validation**

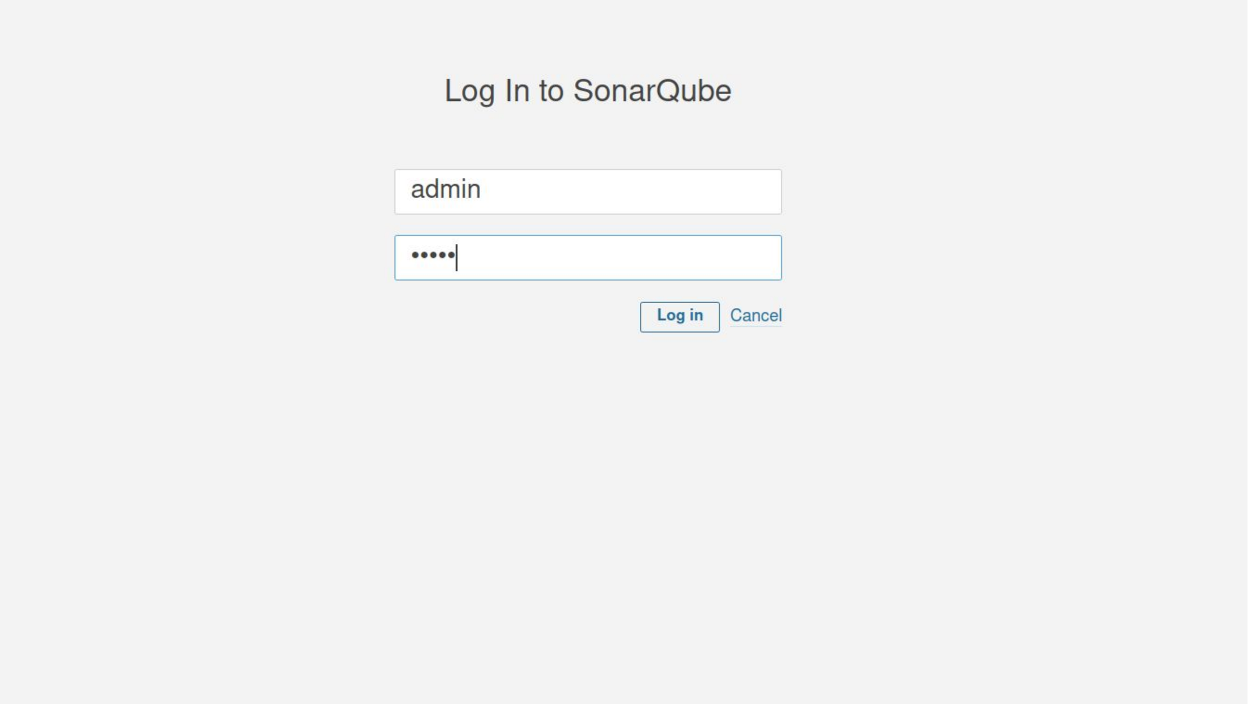
3. Sonarqube

a. Start sonarqube



```
ajay@ajay-Predator-PH315-51:~/Downloads/sonarqube-7.9.5/bin/linux-x86-64$ ./sonar.sh console
Running SonarQube...
wrapper  | --> Wrapper Started as Console
wrapper  | Launching a JVM...
jvm 1    | Wrapper (Version 3.2.3) http://wrapper.tanukisoftware.org
jvm 1    |   Copyright 1999-2006 Tanuki Software, Inc.  All Rights Reserved.
jvm 1    |
jvm 1    | 2021.01.29 20:07:39 INFO  app[][o.s.a.AppFileSystem] Cleaning or creating temp directory /home/ajay/Downloads/sonarqube-7.9.5/temp
jvm 1    | 2021.01.29 20:07:39 INFO  app[][o.s.a.es.EsSettings] Elasticsearch listening on /127.0.0.1:9001
jvm 1    | 2021.01.29 20:07:39 INFO  app[][o.s.a.ProcessLauncherImpl] Launch process[[key='es', ipcIndex=1, logFilenamePrefix=es]] from [/home/ajay/Downloads/sonarqube-7.9.5/elasticsearch]: /home/ajay/Do
wnloads/sonarqube-7.9.5/elasticsearch/bin/elasticsearch
jvm 1    | 2021.01.29 20:07:39 INFO  app[][o.s.a.SchedulerImpl] Waiting for Elasticsearch to be up and running
jvm 1    | OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in version 9.0 and will likely be removed in a future release.
jvm 1    | 2021.01.29 20:07:39 INFO  app[][o.e.p.PluginsService] no modules loaded
jvm 1    | 2021.01.29 20:07:39 INFO  app[][o.e.p.PluginsService] loaded plugin [org.elasticsearch.transport.Netty4Plugin]
jvm 1    | 2021.01.29 20:07:46 INFO  app[][o.s.a.SchedulerImpl] Process[es] is up
jvm 1    | 2021.01.29 20:07:46 INFO  app[][o.s.a.ProcessLauncherImpl] Launch process[[key='web', ipcIndex=2, logFilenamePrefix=web]] from [/home/ajay/Downloads/sonarqube-7.9.5]: /usr/lib/jvm/java-11-open
jdk-amd64/bin/java -Djava.awt.headless=true -Dfile.encoding=UTF-8 -Djava.io.tmpdir=/home/ajay/Downloads/sonarqube-7.9.5/temp --add-opens=java.base/java.util=ALL-UNNAMED --add-opens=java.base/java.lang=AL
L-UNNAMED --add-opens=java.base/java.io=ALL-UNNAMED --add-opens=java.rmi/sun.rmi.transport=ALL-UNNAMED -Xmx512m -Xms128m -XX:+HeapDumpOnOutOfMemoryError -Dhttp.nonProxyHosts=localhost|127.*|[::1] -cp ./l
ib/common/*:/home/ajay/Downloads/sonarqube-7.9.5/lib/jdbc/h2/h2-1.3.176.jar org.sonar.server.app.WebServer /home/ajay/Downloads/sonarqube-7.9.5/temp/sq-process13435040282253472944properties
jvm 1    | 2021.01.29 20:08:34 INFO  app[][o.s.a.SchedulerImpl] Process[web] is up
jvm 1    | 2021.01.29 20:08:34 INFO  app[][o.s.a.ProcessLauncherImpl] Launch process[[key='ce', ipcIndex=3, logFilenamePrefix=ce]] from [/home/ajay/Downloads/sonarqube-7.9.5]: /usr/lib/jvm/java-11-openjd
k-amd64/bin/java -Djava.awt.headless=true -Dfile.encoding=UTF-8 -Djava.io.tmpdir=/home/ajay/Downloads/sonarqube-7.9.5/temp --add-opens=java.base/java.util=ALL-UNNAMED -Xmx512m -Xms128m -XX:+HeapDumpOnOut
OfMemoryError -Dhttp.nonProxyHosts=localhost|127.*|[::1] -cp ./lib/common/*:/home/ajay/Downloads/sonarqube-7.9.5/lib/jdbc/h2/h2-1.3.176.jar org.sonar.ce.app.CeServer /home/ajay/Downloads/sonarqube-7.9.5/
temp/sq-process8163584272311590863properties
jvm 1    | 2021.01.29 20:08:37 INFO  app[][o.s.a.SchedulerImpl] Process[ce] is up
jvm 1    | 2021.01.29 20:08:37 INFO  app[][o.s.a.SchedulerImpl] SonarQube is up
```

b. Login

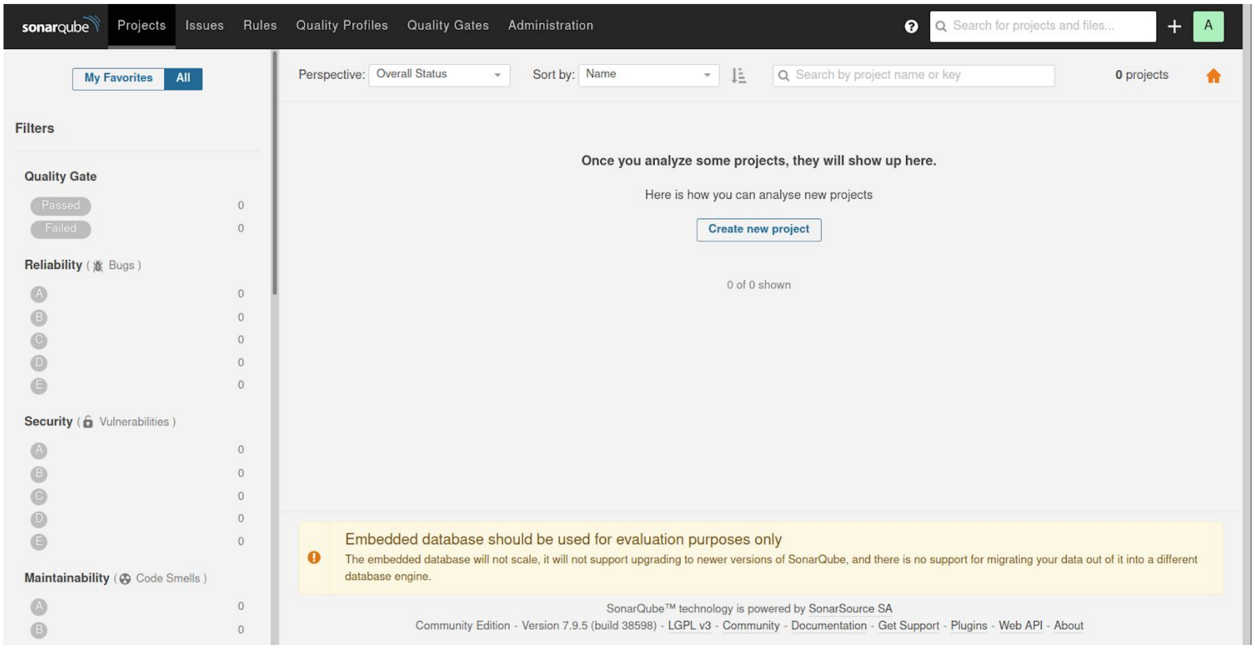


Log In to SonarQube

admin

•••••

c. Create a new project



Once you analyze some projects, they will show up here.

Here is how you can analyse new projects

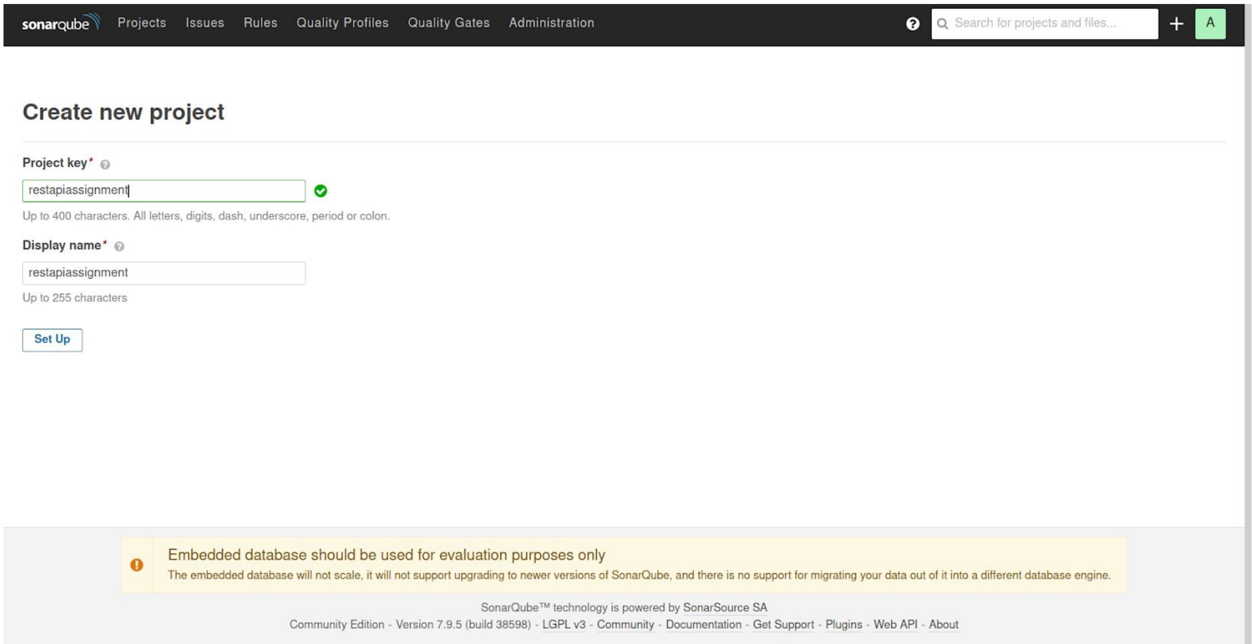
0 of 0 shown

Embedded database should be used for evaluation purposes only

The embedded database will not scale, it will not support upgrading to newer versions of SonarQube, and there is no support for migrating your data out of it into a different database engine.

SonarQube™ technology is powered by SonarSource SA
Community Edition - Version 7.9.5 (build 38598) - LGPL v3 - Community - Documentation - Get Support - Plugins - Web API - About

d. Project key



Create new project

Project key* restapiassignment

Up to 400 characters. All letters, digits, dash, underscore, period or colon.

Display name* restapiassignment

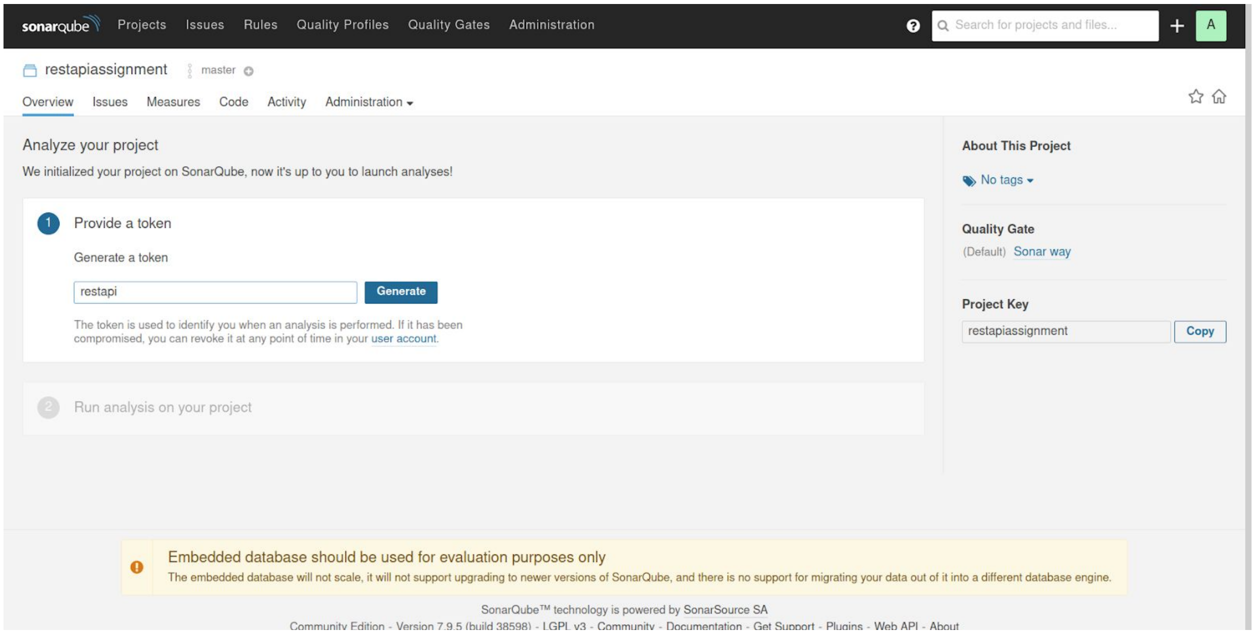
Up to 255 characters

Embedded database should be used for evaluation purposes only

The embedded database will not scale, it will not support upgrading to newer versions of SonarQube, and there is no support for migrating your data out of it into a different database engine.

SonarQube™ technology is powered by SonarSource SA
Community Edition - Version 7.9.5 (build 38598) - LGPL v3 - Community - Documentation - Get Support - Plugins - Web API - About

e. Project token



Analyze your project

We initialized your project on SonarQube, now it's up to you to launch analyses!

1 Provide a token

Generate a token

restapi

The token is used to identify you when an analysis is performed. If it has been compromised, you can revoke it at any point of time in your user account.

2 Run analysis on your project

About This Project

No tags

Quality Gate
(Default) Sonar way

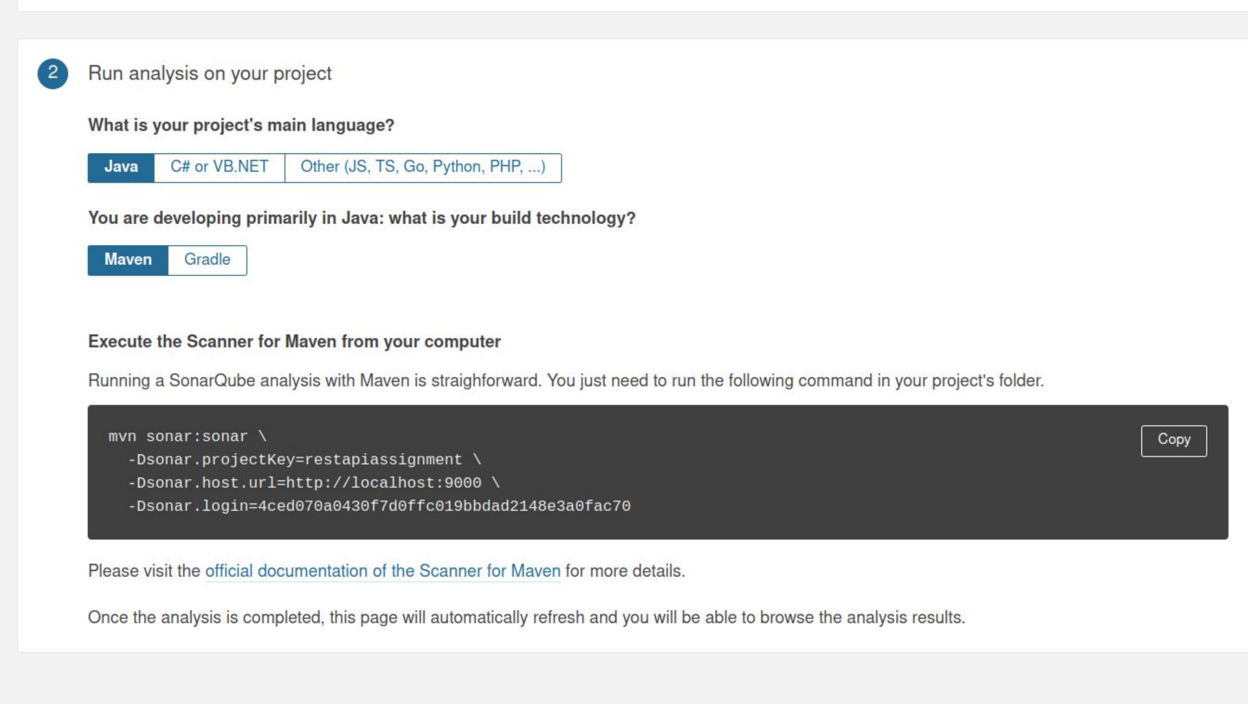
Project Key
restapiassignment

Embedded database should be used for evaluation purposes only

The embedded database will not scale, it will not support upgrading to newer versions of SonarQube, and there is no support for migrating your data out of it into a different database engine.

SonarQube™ technology is powered by SonarSource SA
Community Edition - Version 7.9.5 (build 38598) - LGPL v3 - Community - Documentation - Get Support - Plugins - Web API - About

f. Project analysis



2 Run analysis on your project

What is your project's main language?

You are developing primarily in Java: what is your build technology?

Execute the Scanner for Maven from your computer

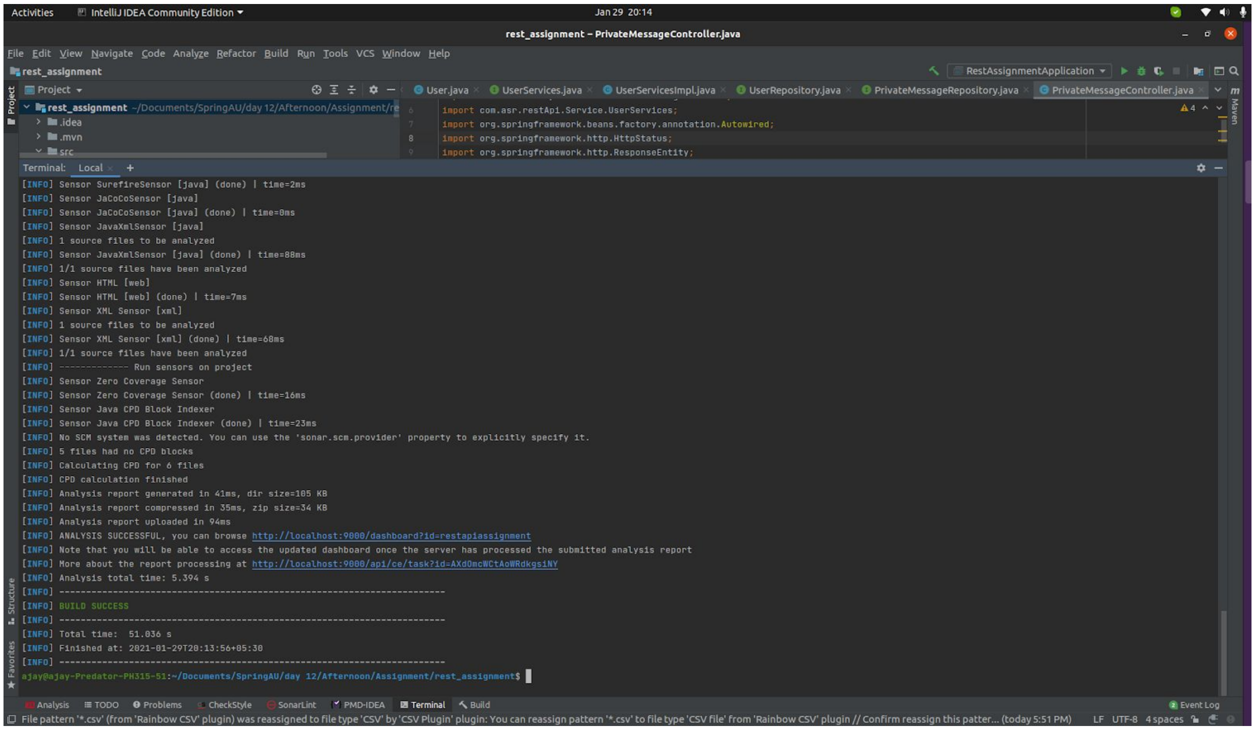
Running a SonarQube analysis with Maven is straighforward. You just need to run the following command in your project's folder.

```
mvn sonar:sonar \
  -Dsonar.projectKey=restapiassignment \
  -Dsonar.host.url=http://localhost:9000 \
  -Dsonar.login=4ced070a0430f7d0ffc019bbdad2148e3a0fac70
```

Please visit the official documentation of the Scanner for Maven for more details.

Once the analysis is completed, this page will automatically refresh and you will be able to browse the analysis results.

g. Analysis execution



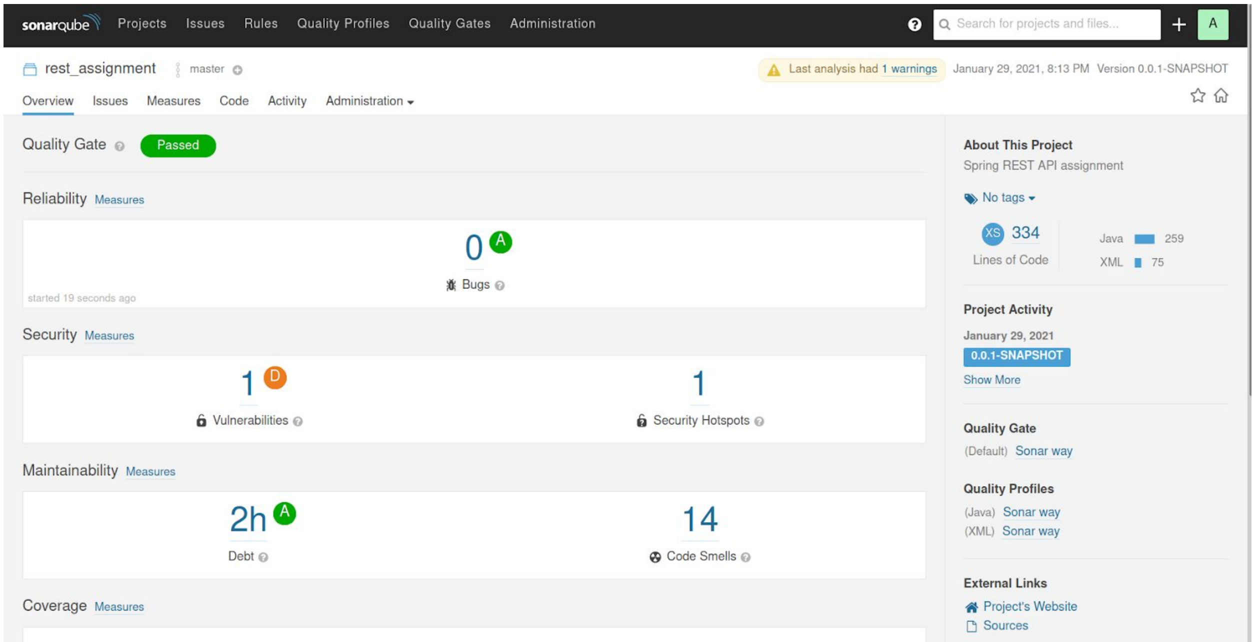
Activities
IntelliJ IDEA Community Edition
Jan 29 20:14
rest_assignment – PrivateMessageController.java
File Edit View Navigate Code Analyze Refactor Build Run Tools VCS Window Help
rest_assignment
RestAssignmentApplication
Project
User.java
UserServices.java
UserServicesImpl.java
UserRepository.java
PrivateMessageRepository.java
PrivateMessageController.java
rest_assignment ~/Documents/SpringAU/day 12/Afternoon/Assignment/re
.idea
.mvn
src
Terminal: Local
Analysis
TODO
Problems
CheckStyle
SonarLint
PMD-IDEA
Terminal
Build
Event Log
LF UTF-8 4 spaces

```
import com.asr.restApi.Service.UserServices;
import org.springframework.beans.factory.annotation.Autowired;
import org.springframework.http.HttpStatus;
import org.springframework.http.ResponseEntity;
```

```
[INFO] Sensor SurefireSensor [java] (done) | time=2ms
[INFO] Sensor JaCoCoSensor [java]
[INFO] Sensor JaCoCoSensor [java] (done) | time=0ms
[INFO] Sensor JavaXmlSensor [java]
[INFO] 1 source files to be analyzed
[INFO] Sensor JavaXmlSensor [java] (done) | time=88ms
[INFO] 1/1 source files have been analyzed
[INFO] Sensor HTML [web]
[INFO] Sensor HTML [web] (done) | time=7ms
[INFO] Sensor XML Sensor [xml]
[INFO] 1 source files to be analyzed
[INFO] Sensor XML Sensor [xml] (done) | time=68ms
[INFO] 1/1 source files have been analyzed
[INFO] ------------- Run sensors on project
[INFO] Sensor Zero Coverage Sensor
[INFO] Sensor Zero Coverage Sensor (done) | time=16ms
[INFO] Sensor Java CPD Block Indexer
[INFO] Sensor Java CPD Block Indexer (done) | time=23ms
[INFO] No SCM system was detected. You can use the 'sonar.scm.provider' property to explicitly specify it.
[INFO] 5 files had no CPD blocks
[INFO] Calculating CPD for 6 files
[INFO] CPD calculation finished
[INFO] Analysis report generated in 41ms, dir size=105 KB
[INFO] Analysis report compressed in 35ms, zip size=34 KB
[INFO] Analysis report uploaded in 94ms
[INFO] ANALYSIS SUCCESSFUL, you can browse http://localhost:9000/dashboard?id=restapiassignment
[INFO] Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report
[INFO] More about the report processing at http://localhost:9000/api/ce/task?id=AXd0mcWCtAoWRdkgsiNY
[INFO] Analysis total time: 5.394 s
[INFO] ------------------------------------------------------------------------
[INFO] BUILD SUCCESS
[INFO] ------------------------------------------------------------------------
[INFO] Total time:  51.036 s
[INFO] Finished at: 2021-01-29T20:13:56+05:30
[INFO] ------------------------------------------------------------------------
ajay@ajay-Predator-PH315-51:~/Documents/SpringAU/day 12/Afternoon/Assignment/rest_assignment$
```

File pattern '*.csv' (from 'Rainbow CSV' plugin) was reassigned to file type 'CSV' by 'CSV Plugin' plugin: You can reassign pattern '*.csv' to file type 'CSV file' from 'Rainbow CSV' plugin // Confirm reassign this patter... (today 5:51 PM)

h. Overview



rest_assignment master

Last analysis had 1 warnings January 29, 2021, 8:13 PM Version 0.0.1-SNAPSHOT

Quality Gate Passed

Reliability Measures

0 A
Bugs

started 19 seconds ago

Security Measures

1 D
Vulnerabilities

1
Security Hotspots

Maintainability Measures

2h A
Debt

14
Code Smells

Coverage Measures

About This Project
Spring REST API assignment

No tags

XS 334
Lines of Code

Java	259
XML	75

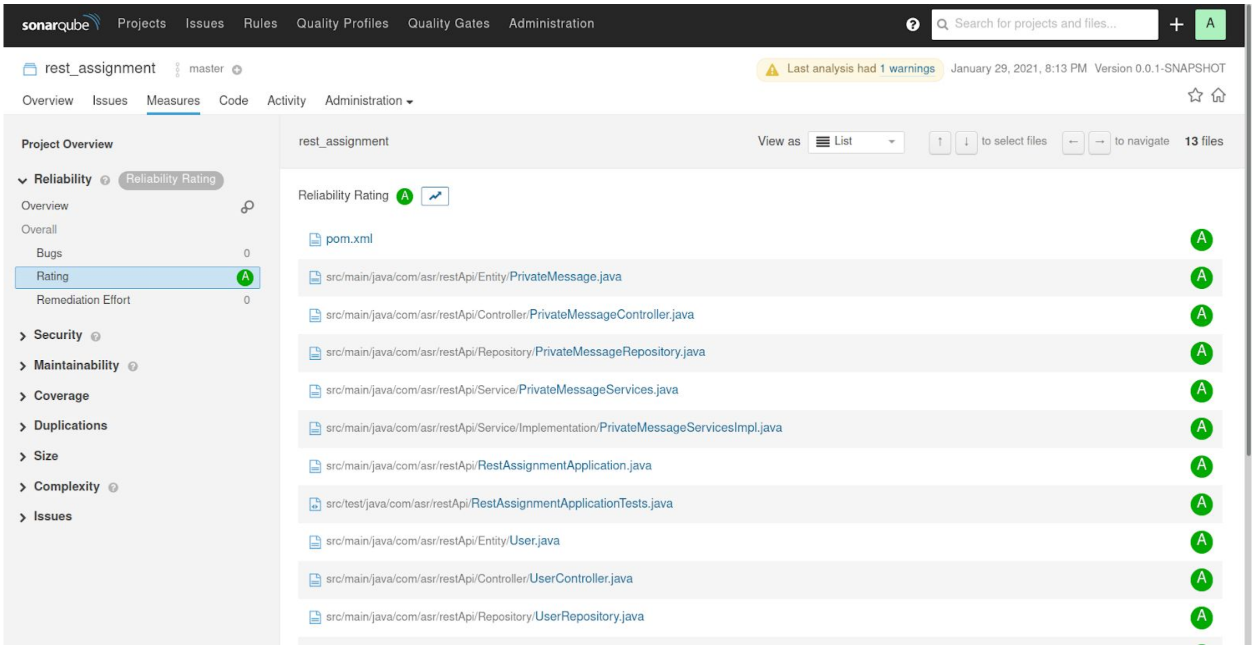
Project Activity
January 29, 2021
0.0.1-SNAPSHOT
Show More

Quality Gate
(Default) Sonar way

Quality Profiles
(Java) Sonar way
(XML) Sonar way

External Links
Project's Website
Sources

i. Rating



rest_assignment master

Last analysis had 1 warnings January 29, 2021, 8:13 PM Version 0.0.1-SNAPSHOT

Project Overview

Reliability Reliability Rating
Overview
Overall

Bugs	0
Rating	A
Remediation Effort	0

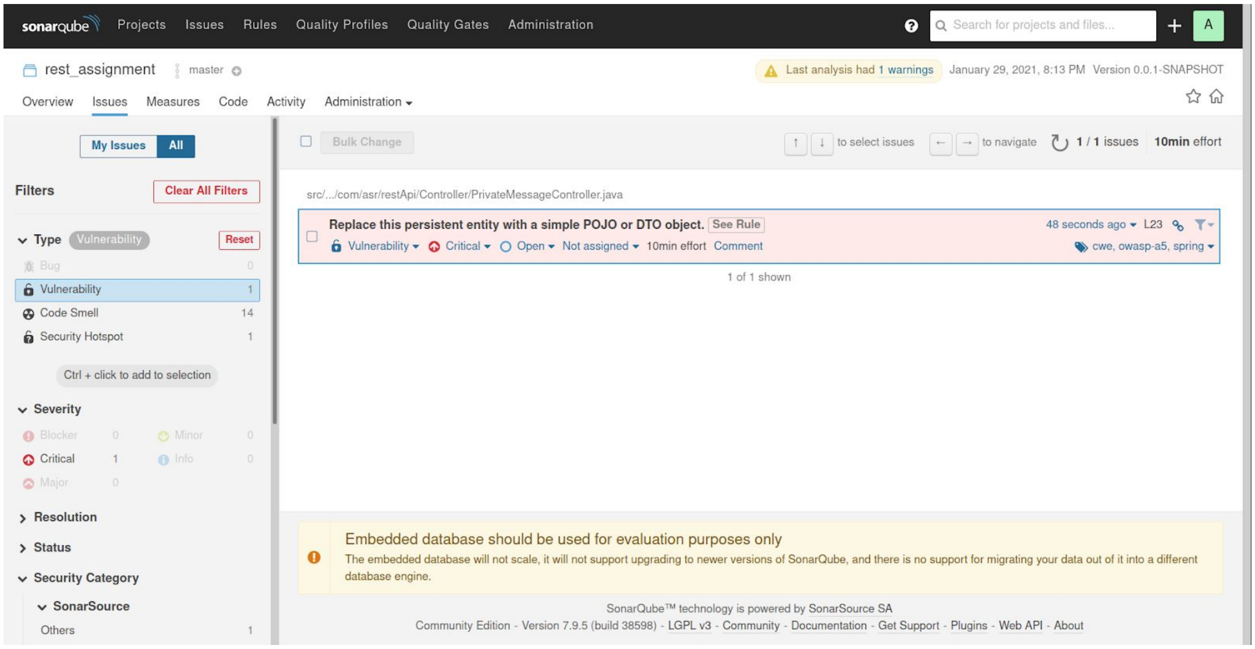
Security
Maintainability
Coverage
Duplications
Size
Complexity
Issues

rest_assignment 13 files

Reliability Rating A

pom.xml	A
src/main/java/com/asr/restApi/Entity/PrivateMessage.java	A
src/main/java/com/asr/restApi/Controller/PrivateMessageController.java	A
src/main/java/com/asr/restApi/Repository/PrivateMessageRepository.java	A
src/main/java/com/asr/restApi/Service/PrivateMessageServices.java	A
src/main/java/com/asr/restApi/Service/Implementation/PrivateMessageServicesImpl.java	A
src/main/java/com/asr/restApi/RestAssignmentApplication.java	A
src/test/java/com/asr/restApi/RestAssignmentApplicationTests.java	A
src/main/java/com/asr/restApi/Entity/User.java	A
src/main/java/com/asr/restApi/Controller/UserController.java	A
src/main/java/com/asr/restApi/Repository/UserRepository.java	A

j. Vulnerability



Last analysis had 1 warnings   January 29, 2021, 8:13 PM   Version 0.0.1-SNAPSHOT

src/.../com/asr/restApi/Controller/PrivateMessageController.java

Replace this persistent entity with a simple POJO or DTO object. See Rule   48 seconds ago   L23
Vulnerability   Critical   Open   Not assigned   10min effort   Comment   cwe, owasp-a5, spring

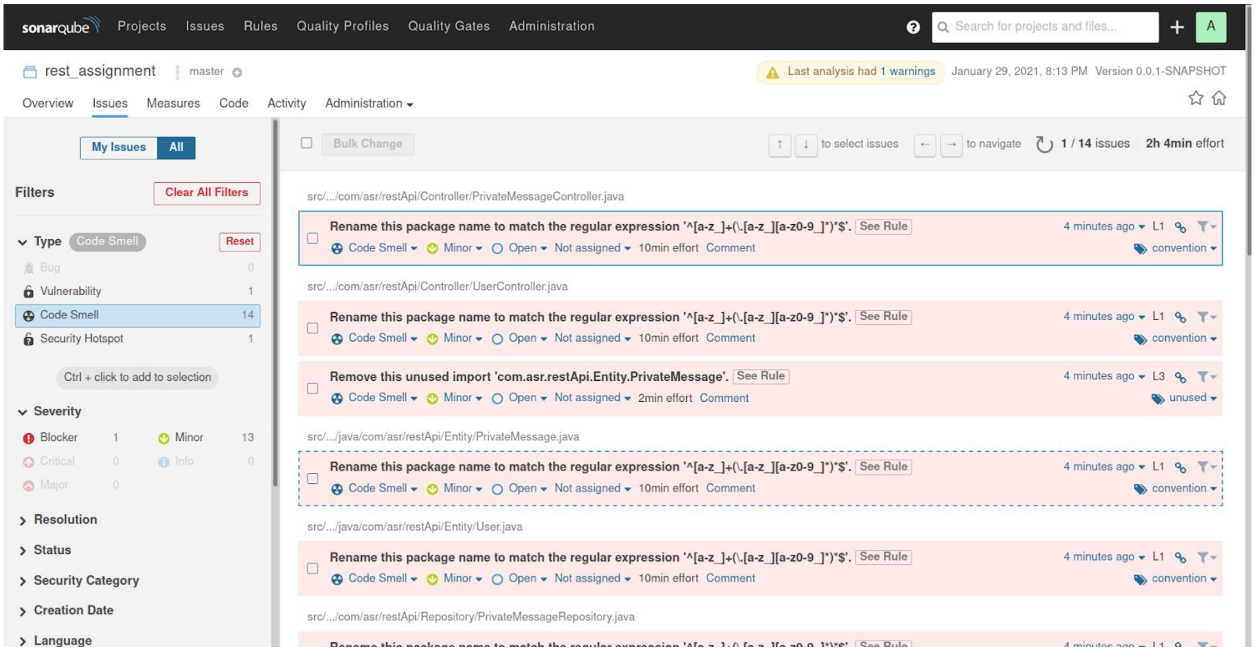
1 of 1 shown

Embedded database should be used for evaluation purposes only

The embedded database will not scale, it will not support upgrading to newer versions of SonarQube, and there is no support for migrating your data out of it into a different database engine.

SonarQube™ technology is powered by SonarSource SA
Community Edition - Version 7.9.5 (build 38598) - LGPL v3 - Community - Documentation - Get Support - Plugins - Web API - About

k. Code smell



Last analysis had 1 warnings   January 29, 2021, 8:13 PM   Version 0.0.1-SNAPSHOT

src/.../com/asr/restApi/Controller/PrivateMessageController.java

Rename this package name to match the regular expression '^[a-z_]+(\.[a-z_][a-z0-9_]*)*$'. See Rule   4 minutes ago   L1
Code Smell   Minor   Open   Not assigned   10min effort   Comment   convention

src/.../com/asr/restApi/Controller/UserController.java

Rename this package name to match the regular expression '^[a-z_]+(\.[a-z_][a-z0-9_]*)*$'. See Rule   4 minutes ago   L1
Code Smell   Minor   Open   Not assigned   10min effort   Comment   convention

Remove this unused import 'com.asr.restApi.Entity.PrivateMessage'. See Rule   4 minutes ago   L3
Code Smell   Minor   Open   Not assigned   2min effort   Comment   unused

src/.../java/com/asr/restApi/Entity/PrivateMessage.java

Rename this package name to match the regular expression '^[a-z_]+(\.[a-z_][a-z0-9_]*)*$'. See Rule   4 minutes ago   L1
Code Smell   Minor   Open   Not assigned   10min effort   Comment   convention

src/.../java/com/asr/restApi/Entity/User.java

Rename this package name to match the regular expression '^[a-z_]+(\.[a-z_][a-z0-9_]*)*$'. See Rule   4 minutes ago   L1
Code Smell   Minor   Open   Not assigned   10min effort   Comment   convention

src/.../com/asr/restApi/Repository/PrivateMessageRepository.java